证　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：2002 03 08

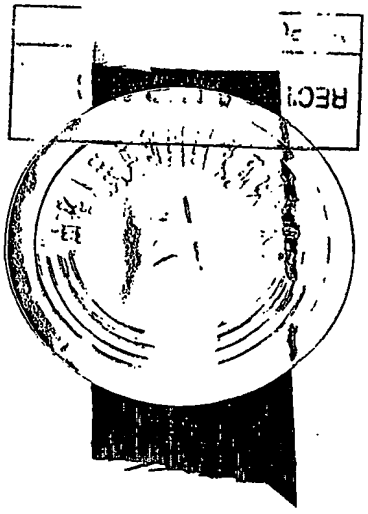
申　请　号：02 1 10974.5

申请类别：发明

发明创造名称：无线局域网加密密钥的分发方法

申　请　人：华为技术有限公司

发明人或设计人：李永茂；吴更石



中华人民共和国
国家知识产权局局长 王景川

2003 年 3 月 11 日

权 利 要 求 书

1.一种无线局域网加密密钥的分发方法，所述无线局域网包含一接入站(AP)和若干存储自身标识信息的移动终端，移动终端通过无线信道与 AP 通信，AP 与外部网络和对移动终端身份进行认证的认证装置连接，所述认证装置存储有各移动终端的标识信息，其特征在于所述方法包含如下步骤：

(1)移动终端向认证装置发送包含标识信息的认证请求以请求对其进行身份认证；

(2)认证装置根据认证请求中包含的标识信息对移动终端进行认证，如果认证失败，则经 AP 向移动终端发送拒绝接入消息；如果认证成功，则认证装置向 AP 发送与密钥有关的信息 M1，并且经 AP 向该移动终端发送包含允许接入通知信息的消息，如果该消息包含与密钥有关的信息 M2，则必须经过加密处理；

(3)AP 根据认证装置向其发送的与密钥有关的信息 M1 获得密钥，移动终端根据认证装置经 AP 向其发送的消息获得密钥。

2.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 为认证装置根据认证请求中包含的标识信息查找到的相应特征信息，AP 获得密钥的方式为根据密钥生成算法从所述特征信息生成密钥，而移动终端获得密钥的方式为在接收到 AP 转发的包含允许接入通知信息的消息后根据同一密钥生成算法从自身存储的所述特征信息生成密钥。

3.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 为认证装置根据认证请求中包含的标识信息查找到的相应特征信息，AP 获得密钥的方式为根据密钥生成算法生成密钥，所述信息 M2 为 AP 获得的密钥并以所述特征信息加密后连同允许接入通知信息一起发送给移动终端，移动终端获得密钥的方式为用所述特征信息对信息 M2 进行解密以获得密钥。

4.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 为认证装置根据密钥生成算法从与认证请求中包含的标识信息对应的特征信息生成的密钥，移动终端获得密钥的方式为在接收到允许接入通知信息后根据同一密钥生成算法从自身存储的所述特征信息生成密钥。

5.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 和 M2 为认证装置根据密钥生成算法从与认证请求中包含的标识信息对应的特征信息生成的密钥，所述信息 M2 以所述特征信息加密后连同允许接入通知信息发送给移动终端，移动终端获得密钥的方式为在接收到允许接入通知信息后以自身存储的所述特征信息对信息 M2 解密获得密钥。

6.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新密钥：

(a1)AP 产生一个随机数并利用任一密钥生成算法从该随机数生成新密钥；

(b1)AP 将该随机数放入改变密钥通知一起发送给移动终端；

(c1)当移动终端收到改变密钥通知后，根据改变密钥通知中包含的随机数，利用与步骤(a)中所述相同的密钥生成算法产生新密钥；

(d1)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e1)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

7.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新通信密钥以完成新密钥下的加密通信：

(a2)AP 以任意方式生成新的密钥并用当前使用的密钥对新生成的密钥进行加密；

(b2)AP 将加密后的密钥放入改变密钥通知一起发送给移动终端；

(c2)当移动终端收到改变密钥通知后，用当前使用的密钥解密包含在改变密钥通知中的新密钥从而获得新密钥；

(d2)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e2)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

8.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新密钥：

(a3)认证装置首先产生一个随机数以利用密钥生成算法从该随机数生成新密钥，然后将新密钥发送给 AP 而将随机数经 AP 发送给移动终端；

(b3)AP 在接收到新密钥之后将改变密钥通知发送给移动终端；

(c3)当移动终端收到认证装置发送的随机数和 AP 发送的改变密钥通知

后，根据随机数，利用与步骤(a)中所述相同的密钥生成算法产生新密钥；

(d3)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e3)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

9.如权利要求 1—5 任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新通信密钥以完成新密钥下的加密通信：

(a4)认证装置以任意方式生成新的密钥并用当前使用的密钥对新生成的密钥进行加密，新密钥被发送给 AP 而加密后的新密钥经 AP 被发送给移动终端；

(b4)AP 接收到新密钥后向移动终端发送改变密钥通知；

(c4)当移动终端收到认证装置发送的加密密钥和 AP 发送的改变密钥通知后，用当前使用的密钥解密加密密钥从而获得新密钥；

(d4)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e4)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

10.如权利要求 1—5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

11.如权利要求 6 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

12.如权利要求 7 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

13.如权利要求 8 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

14.如权利要求 9 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

15.如权利要求 1—5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

16.如权利要求 6 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

17.如权利要求 7 所述的无线局域网加密密钥的分发方法，其特征在于所

述认证装置为将外部网络与 AP 连接起来的无线网关。

18.如权利要求 8 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

19.如权利要求 9 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

20.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

21.如权利要求 6 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

22.如权利要求 7 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

23.如权利要求 8 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

24.如权利要求 9 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

02.03.15

9

说　明　书

无线局域网加密密钥的分发方法

发明领域

本发明涉及无线局域网内接入站(AP)与移动终端之间的通信，特别涉及加密密钥的分发方法。

背景技术

无线局域网借助无线信道传输数据、话音和视频信号。相对于传统布线网络，无线局域网具有安装便捷、使用灵活、经济节约和易于扩展等优点，因而日益受到重视。

无线局域网的可覆盖区域称为服务区域，一般分为基本服务区域(Basic Service Area，以下简称为 BSA)和扩展服务区域(Extended Service Area，以下简称为 ESA)，其中 BSA 指由无线局域网中各单元的无线收发机以及地理环境所确定的通信覆盖区域，常称为小区(cell)，范围一般较小；为了扩大无线局域网覆盖区域，通常采用如图 1 所示的方法，即通过接入站(Access Point，以下简称为 AP)经无线网关将 BSA 与骨干网(通常是有线局域网)相连接，使多个 BSA 中的移动终端 MH 经由 AP 和无线网关与有线骨干网连接，从而构成扩展服务区域。

与有线传输相比，无线传输的保密性较差，因此为了保证小区内 AP 与移动终端之间的通信安全，信息必须用密钥加密以后才能发送。当移动终端跨区移动或加电启动时，首先应寻找自己所在的小区，向该小区的 AP 登录，并获得该小区的相关信息，因此其与 AP 的加密通信将受到一定的限制。具体而言，例如当移动终端 MH12 从小区 1 进入小区 2 时，如果 AP11 与 AP21 属于同一密钥管理服务器的覆盖范围，则移动终端 MH12 与 AP11 的加密通信可以顺利过渡至其与 AP21 的加密通信而不受影响，但是如果 AP11 与 AP21 分属不同的密钥管理服务器，则由于 AP21 无法获知移动终端 MH12 的通信密钥，所以无法在小区 2 内直接实现移动终端 MH12 与 AP21 的加密通信。而如果由移动终端 MH12 将密钥以非加密方式通过无线信道发送给 AP21 来实现加密通信，则由于密钥容易被截获和破译，所以系统存在很大的安全隐患。

由上可见，现有技术下加密密钥的分发方法存在移动终端跨区漫游时加密通信受到限制的缺点。

发明内容

02.03.15 .10

针对上述情况，本发明提出一种新的无线局域网加密密钥的分发方法。

按照本发明的无线局域网加密密钥的分发方法，所述无线局域网包含一接入站(AP)和若干存储自身标识信息的移动终端，移动终端通过无线信道与 AP 通信，AP 与外部网络和对移动终端身份进行认证的认证装置连接，所述认证装置存储有各移动终端的标识信息，所述方法包含如下步骤：

(1)移动终端向认证装置发送包含标识信息的认证请求以请求对其进行身份认证；

(2)认证装置根据认证请求中包含的标识信息对移动终端进行认证，如果认证失败，则经 AP 向移动终端发送拒绝接入消息；如果认证成功，则认证装置向 AP 发送与密钥有关的信息 M1，并且经 AP 向该移动终端发送包含允许接入通知信息的消息，如果该消息包含与密钥有关的信息 M2，则必须经过加密处理；

(3)AP 根据认证装置向其发送的与密钥有关的信息 M1 获得密钥，移动终端根据认证装置经 AP 向其发送的消息获得密钥。

由上可见，本发明的利用密钥的通信方法将密钥的分发过程与移动终端的认证过程结合在一起，利用认证装置对密钥分发进行管理，因此，移动终端用户可以在大于密钥管理服务器覆盖范围内跨区漫游。由于密钥的分发不涉及通过空中接口中传递未加密的密钥，所以保证了密钥安全。此外，上述密钥分配方法不依赖于特定的认证方式，因而可以在各种无线局域网协议下实现。最后，由于 AP 无需管理用户信息，简化了 AP 的结构从而降低了成本。

附图说明

通过以下结合附图对本发明实施例的描述，可以进一步理解本发明的各种优点、特点和特征，其中：

图 1 为无线局域网经 AP 和无线网关与有线骨干网连接的示意图；

图 2a 为按照本发明一个实施例的无线局域网内加密通信方法的示意图；

图 2b 为按照本发明另一实施例的无线局域网内加密通信方法的示意图；

图 2c 为按照本发明另一实施例的无线局域网内加密通信方法的示意图；

图 2d 为按照本发明另一实施例的无线局域网内加密通信方法的示意图；

图 3a 示出了无线局域网内动态协商密钥的一个实例过程；

图 3b 示出了无线局域网内动态协商密钥的另一个实例过程；

图 3c 示出了无线局域网内动态协商密钥的另一个实例过程；

图 3d 示出了无线局域网内动态协商密钥的另一个实例过程；以及

图 4 为 IEEE 802.1x 协议下 MAC 帧结构的示意图。

具体实施方式

以下首先借助图 1、图 2a—2d 描述按照本发明实施例的无线局域网内加密密钥的分发方法。

如图 1 所示，小区 1~3 包含一接入站 AP11、AP21 和 AP31 以及若干移动终端 MH12~MH33，每个移动终端都存储有标识其身份的身份信息 I 和特征信息 P，每个移动终端通过无线信道与同属一个小区内的 AP 通信，AP 经无线网关 51-53 与有线骨干网 4 连接，骨干网内的认证服务器(未画出)包含了所有小区内的所有移动终端的身份信息 I 和特征信息 P，认证服务器也可以从外部设备获得存储每个移动终端身份信息 I 和特征信息 P 的用户列表，因此可以利用其存储的或用户列表提供的身份信息 I 对任一移动终端用户的身份进行确认。值得指出的是，移动终端的身份信息 I 和特征信息 P 也可以由无线网关 51-53 存储或管理，由此可由无线网关实现对移动终端用户身份的认证功能。另外，还可以由认证服务器与无线网关协同实现对移动终端用户身份的确认功能。对于本领域内的技术人员来说，实现移动终端用户的身份确认功能的方式是公知的并且可以有多种，利用认证服务器和/或无线网只是其中的几种方式，为方便表述起见，以下将具有移动终端用户身份确认功能的装置统称为认证装置。

图 2a 示出了移动终端 MH12 从小区 1 进入小区 2 时其与 AP21 之间通信用密钥的首次分发过程和加密通信过程。

移动终端 MH12 首先与 AP21 建立初始连接，经 AP21 和无线网关 51 向骨干网 4 内的认证服务器发送包含身份信息的认证请求以请求对其进行认证。认证服务器在接收到认证请求后，首先根据认证请求中包含的身份信息 I 对移动终端的身份进行认证，如果发现所包含的身份信息 I 与其存储的不相符，则判断移动终端用户为非法用户，认证请求无效，因此经无线网关 51 和 AP21 向移动终端 MH11 发送拒绝接入消息。如果发现认证请求所包含的身份信息 I 与其存储的相符，则判断移动终端用户为合法用户，认证请求有效，因此如图 2a 所示，认证服务器根据包含的身份信息 I 查找对应移动终端 MH12 的特征信息 P 并将查找到的特征信息 P 经无线网关 51 发送给 AP21。AP21 在接收到认证服务器发送的特征信息 P 之后经无线网关向认证服务器返回确认收到特征信息 P 的确认消息并根据密钥生成算法从特征信息 P 生成密钥。密钥生成算法可以是任意一种算法，并且密钥的长度是任意的。认证服务器在接收到 AP21 发送的确认消息之后即经无线网关 51 和 AP21 向移动终端 MH21 发送允许接入通知消息。移动终端 MH21 收到允许接入通知消息之后，根据与 AP21 生成密钥时所用的相同算法，从其自身存储的特征信息 P 生成密钥以用该密钥对发送至 AP21 的数据分组进行加密并向 AP21 发送，移动终端 MH21 在对数据分组进行加密时在数据分组内加入加密标识。AP21 在收到移动终端 MH21 发送的数据分组后，首先检测数据分组中的加密标识，如果检测到加密

标识，则使用根据密钥生成算法从特征信息 P 得到的密钥对数据分组解密并经无线网关 51 转发至外部网络 4，否则将数据分组经无线网关 51 直接转发外部网络 4。

图 2b 为按照本发明另一实施例的无线局域网内加密通信方法的示意图。该实施例与图 2a 所示实施例的区别在于，在上述通信过程中，密钥由 AP21 利用任一密钥生成算法生成并用特征信息 P 对密钥加密后发送给移动终端 MH21。移动终端 MH21 在接收到 AP21 发送的密钥之后，用其自身存储的特征信息 P 对密钥进行解密，然后用解密后的密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时在数据分组内也加入加密标识。在这种情况下，各移动终端无需知晓 AP21 所采用的密钥生成算法。

图 2c 为按照本发明另一实施例的无线局域网内加密通信方法的示意图。该实施例与图 2a 所示实施例的区别在于，当认证成功时，认证服务器可以根据密钥生成算法从查找到的特征信息 P 生成密钥并发送给 AP21 而不是将特征信息 P 发送给 AP21 供其生成密钥。

图 2d 为按照本发明另一实施例的无线局域网内加密通信方法的示意图。该实施例与图 2c 所示实施例的区别在于，当认证成功时，认证服务器可以根据密钥生成算法生成密钥并发送给 AP21，与此同时认证服务器还向移动终端 MH21 发送以特征信息 P 加密的密钥。

值得指出的是，骨干网 4 内可以包含若干台认证服务器，它们之间通过一定的通信协议连接以交换所存储的移动终端的标识信息，因此可以进一步扩大扩展服务区域。

在上述实施例中，如果移动终端用户身份的确认功能由无线网关 51－53 单独实现，则原先认证服务器所实现的其它功能也可以由无线网关实现，例如可以由无线网关 51－53 向移动终端 MH21 发送允许接入通知，生成密钥以及向 AP21 发送特征信息 P 等。同样，如果确认功能由认证服务器与无线网关协同实现，则原先认证服务器所实现的其它功能可以由认证服务器与无线网关协同实现。总之，原先认证服务器所实现的全部功能都可以由认证装置实现。

在上述无线局域网内加密通信过程中，为了进一步提高系统的安全性，AP 与移动终端之间的通信密钥还可定期或不定期动态更新。以下借助图 3a－3d 描述这种动态协商密钥的几个实例过程。

如图 3a 所示，为了更换密钥，首先由 AP 产生一个随机数，并利用任一密钥生成算法从该随机数生成密钥，随后 AP 将该随机数放入改变密钥通知一起发送给移动终端。当移动终端收到改变密钥通知后，就根据改变密钥通知中包含的随机数，利用相同的密钥生成算法产生密钥，随后用该密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时

仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

图 3b 示出了另一动态协商密钥的实例过程，在图 3b 中，为了更换密钥，首先由 AP 以任意方式生成新的密钥，随后 AP 用当前密钥对新生成的密钥进行加密并将加密后的密钥放入改变密钥通知一起发送给移动终端。当移动终端收到改变密钥通知后，用当前密钥解密包含在改变密钥通知中的新密钥，随后用该新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

图 3c 示出了另一动态协商密钥的实例过程，在图 3c 中，为了更换密钥，首先由认证装置产生一个随机数，并利用任一密钥生成算法从该随机数生成密钥，随后认证装置将该随机数发送给移动终端并将生成的密钥发送给 AP。当 AP 收到认证装置发送的密钥之后，向移动终端发送改变密钥通知。当移动终端收到改变密钥通知和随机数后，利用相同的密钥生成算法产生密钥，随后用该密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

图 3d 示出了另一动态协商密钥的实例过程，在图 3d 中，为了更换密钥，首先由认证装置以任意方式生成新的密钥，随后认证装置将密钥发送给 AP 并用当前密钥对新生成的密钥进行加密后发送给移动终端。AP 在接收到认证装置发送的未加密密钥后向移动终端发送改变密钥通知。当移动终端收到改变密钥通知和加密的密钥后，用当前密钥解密加密密钥以得到新密钥，随后用该新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

在上述动态协商密钥过程中，如果 AP 在发出改变密钥通知以后，发现移动终端发送的数据分组内加密标识的数值未作改变，则再次发送改变密钥通知和随机数或加密的新密钥，直到移动终端启用新的密钥进行通信。

由上可见，上述密钥分配方法并不涉及无线局域网内登录管理、认证管理和移动管理的特定方式，因此可以在各种无线局域网协议体系下实现，包括 PPPoE、IEEE 802.1x 协议等。但是为了进一步理解本发明的特点、优点和目标，以下以 IEEE 802.1x 协议为例描述本发明密钥分配方法的具体实现方式。

IEEE 802.1x 是一种常用的无线局域网的协议体系，涉及 MAC 层和物理层标准，AP 与移动终端之间的数据分组以 MAC 帧为单位，图 4 示出了典型的 MAC 帧结构。IEEE 802.1x 协议报文主要包括 EAP_START、EAP_LOGOOF、EAP_REQUEST、EAP_RESPONSE、EAP_SUCCESS、EAP_FAIL 和 EAP_KEY，

这些报文为特殊的 MAC 帧，都通过 MAC 帧中的类型域来标识。

当移动终端与 AP 之间初始连接时，首先移动终端向 AP 发送 EAP_START 报文，AP 在收到后向移动终端发送 EAP_REQUEST/IDENTITY 报文，要求用户输入用户名和密码。用户输入用户名和密码，移动终端将它们封装在 EAP_RESPONSE/IDENTITY 报文中并回送给 AP。AP 将用户提供的用户名和密码信息封装在 Access_Request 报文中发送给认证服务器，AP 与认证服务器之间的通信遵循 Radius 协议。认证服务器首先验证用户名和密码是否匹配，如果不匹配，则确定认证失败并将 Accept-Reject 报文回送给 AP。AP 收到后发送 EAP_FAIL 报文给移动终端，拒绝移动终端接入。如果认证成功，则认证服务器发送 Access_Accept 报文，同时在该报文的数据域中包含该用户的对应信息 P。AP 收到该消息后，如上述密钥分配方法所述，既可以根据某一密钥生成算法从对应信息 P 生成密钥并发送 EAP_SUCCESS 报文给移动终端，也可以用对应信息 P 加密生成的密钥然后借助 EAP_KEY 报文传送给移动终端。相应地，移动终端可根据同样的密钥生成算法从自己存储的对应信息 P 生成密钥或者用对应信息 P 解密接收到的密钥。接着，移动终端使用密钥对 MAC 帧数据进行加密并传送给 AP，同时在 MAC 帧中加入加密标识。如图 4 所示，帧体域由 IV 域、数据域和 ICV 域组成，特别是在 IV 域中包含了 2 个比特的 KeyID 域作为同步标志。比较好的是，当 MAC 帧未加密时，KeyID=0，当开始加密通信时，每次改变密钥，KeyID 都递增 1，即 KeyID=KeyID+1。如果 KeyID=3，则再次更新密钥时将 KeyID 重置为 1 而不是 0。因此首次加密 MAC 数据时，移动终端发出的 MAC 帧中的域 KeyID=1。AP 在收到 KeyID＝1 的 MAC 帧后，确定移动终端已启用新分配的密钥，于是就用前述生成的密钥解密 MAC 数据，并且转换为以太网格式向有线网络转发。如果 AP 在发送 EAP_KEY 报文后，发现移动终端上传的 MAC 帧中的 KeyID 域仍然为 0，则重发 EAP_SUCCESS 报文或者 EAP_KEY。

为了动态地更新通信密钥，AP 可以自移动终端登录起，定期(例如每隔 10 分钟)或不定期地发送 EAP_KEY 报文，通知移动终端修改密钥。在发送的 EAP_KEY 中，可选择包含生成密钥所用的随机数或者用当前密钥加密的新密钥。移动终端在收到该报文后，可以用相同的密钥生成方法从该随机数生成新密钥或者用当前密钥解密新的密钥。接着，移动终端用新密钥加密 MAC 数据，同时使 KeyID 取值为 KeyID＝2。AP 检测上传的 MAC 帧的 KeyID 域，如果 KeyID 保持不变，则继续使用当前密钥解密 MAC 数据，同时重发 EAP_KEY 报文。如果 KeyID 改变，则使用新密钥解密 MAC 数据。

15

说 明 书 附 图

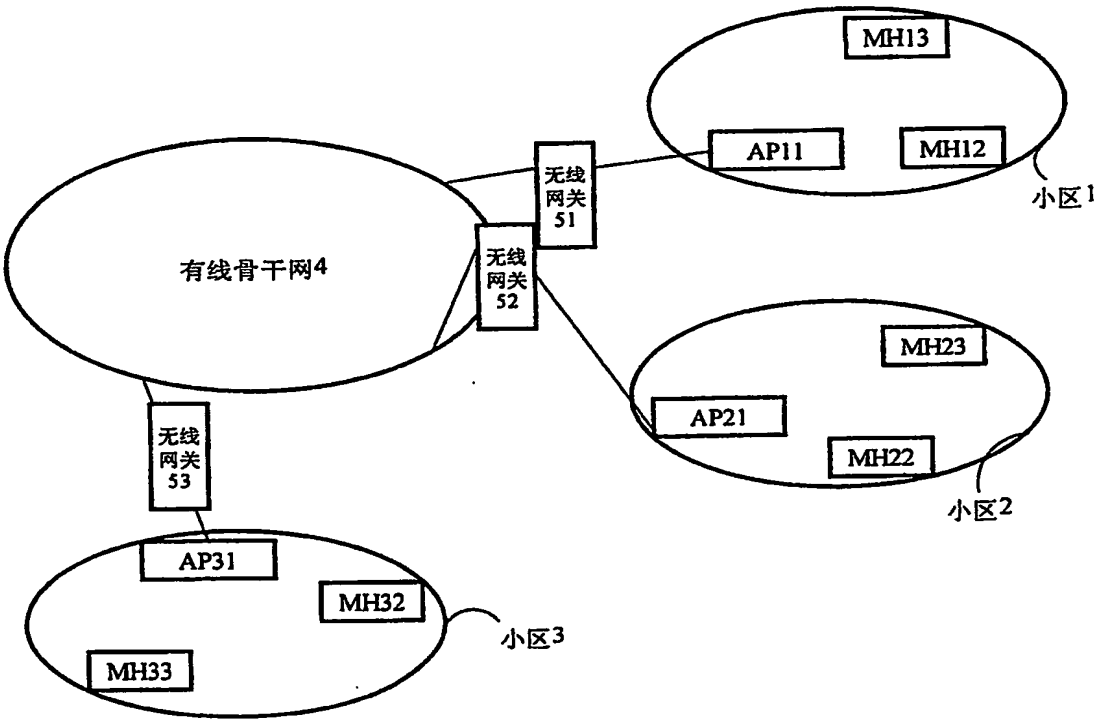

MH13
AP11
MH12
小区1
无线网关51
无线网关52
有线骨干网4
MH23
AP21
MH22
小区2
无线网关53
AP31
MH32
小区3
MH33

图 1

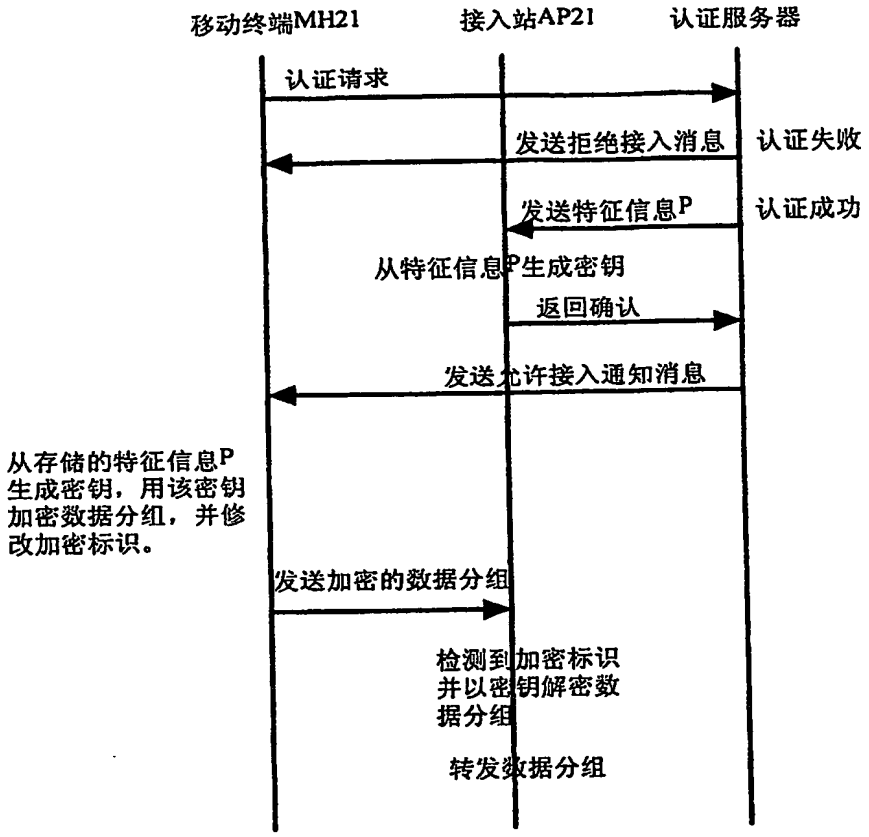

移动终端MH21
接入站AP21
认证服务器
认证请求
发送拒绝接入消息
认证失败
发送特征信息P
认证成功
从特征信息P生成密钥
返回确认
发送允许接入通知消息
从存储的特征信息P生成密钥，用该密钥加密数据分组，并修改加密标识。
发送加密的数据分组
检测到加密标识并以密钥解密数据分组
转发数据分组

图 2a

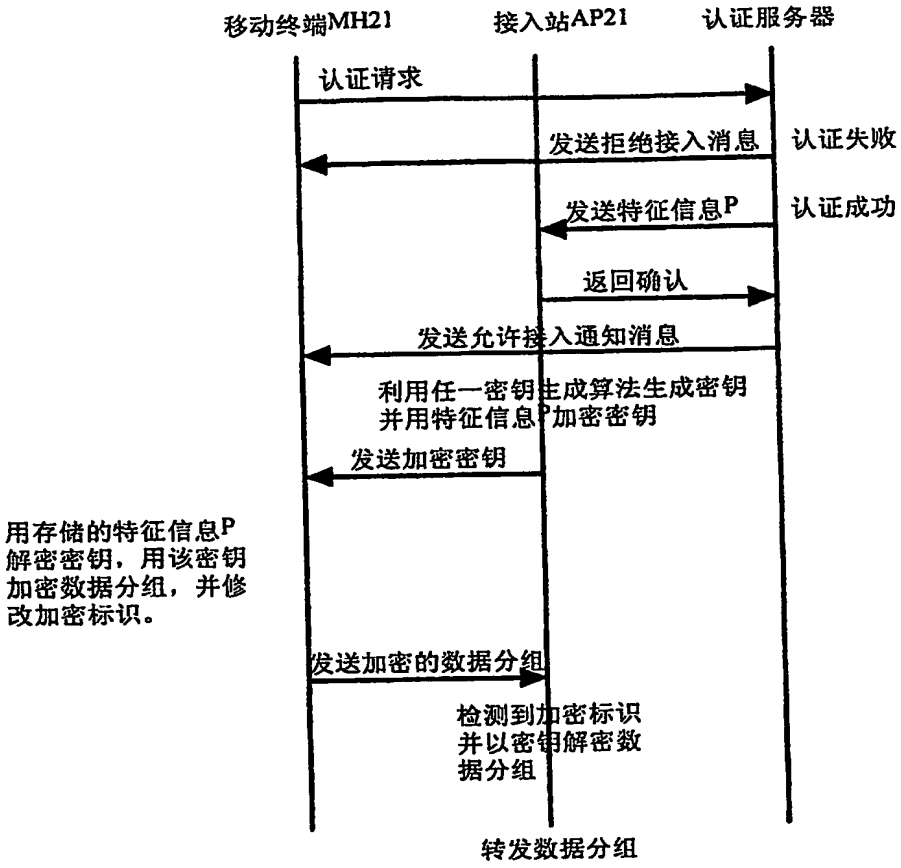

移动终端MH21
接入站AP21
认证服务器
认证请求
发送拒绝接入消息
认证失败
发送特征信息P
认证成功
返回确认
发送允许接入通知消息
利用任一密钥生成算法生成密钥
并用特征信息P加密密钥
发送加密密钥
用存储的特征信息P
解密密钥，用该密钥
加密数据分组，并修
改加密标识。
发送加密的数据分组
检测到加密标识
并以密钥解密数
据分组
转发数据分组

图 2b

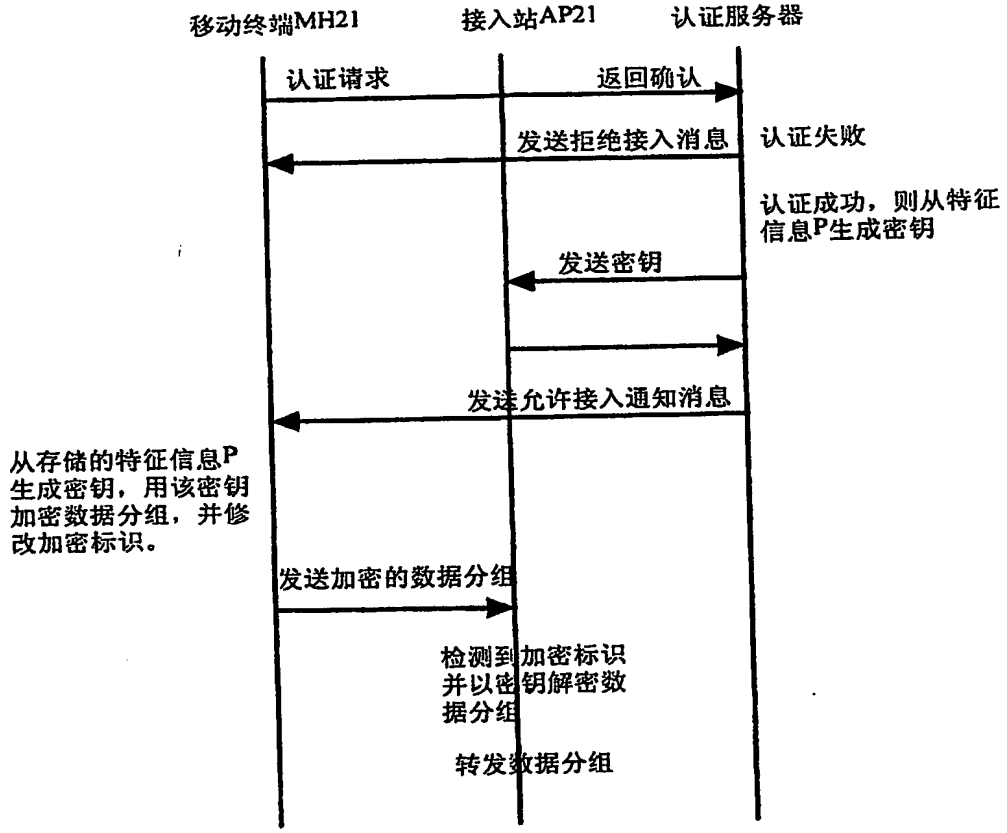

移动终端MH21
接入站AP21
认证服务器
认证请求
返回确认
发送拒绝接入消息
认证失败
认证成功，则从特征信息P生成密钥
发送密钥
发送允许接入通知消息
从存储的特征信息P生成密钥，用该密钥加密数据分组，并修改加密标识。
发送加密的数据分组
检测到加密标识并以密钥解密数据分组
转发数据分组

图 2c

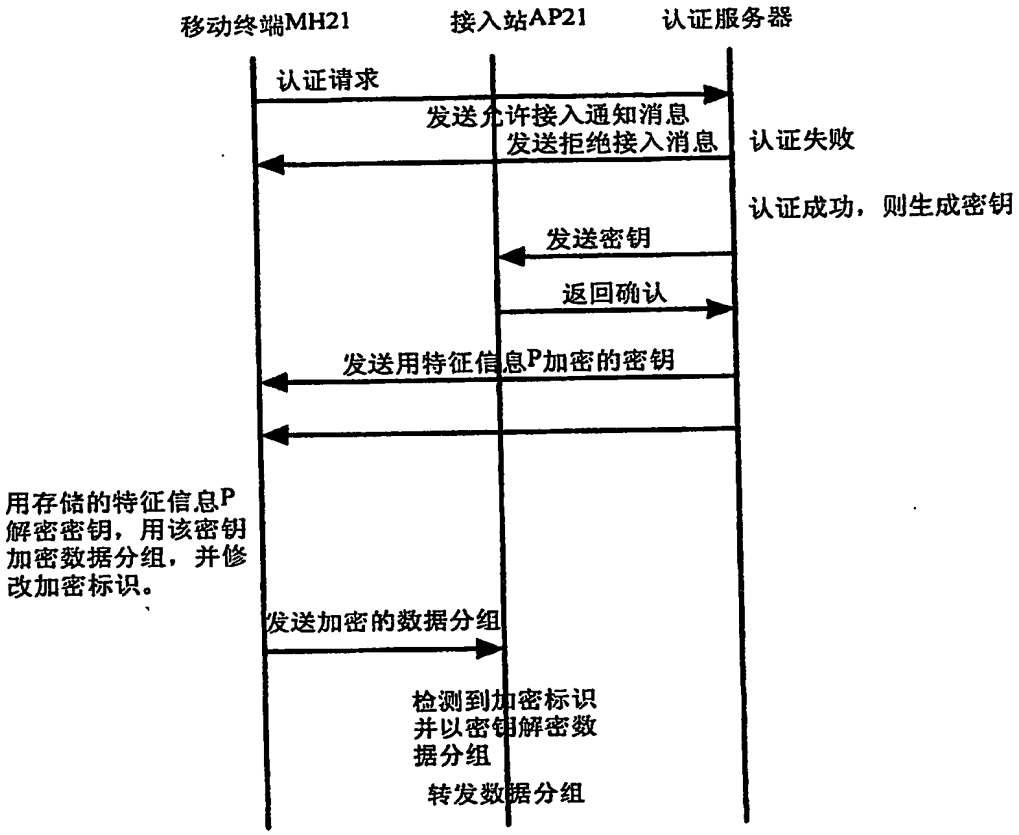

移动终端MH21
接入站AP21
认证服务器
认证请求
发送允许接入通知消息
发送拒绝接入消息
认证失败
认证成功，则生成密钥
发送密钥
返回确认
发送用特征信息P加密的密钥
用存储的特征信息P解密密钥，用该密钥加密数据分组，并修改加密标识。
发送加密的数据分组
检测到加密标识并以密钥解密数据分组
转发数据分组

图 2d

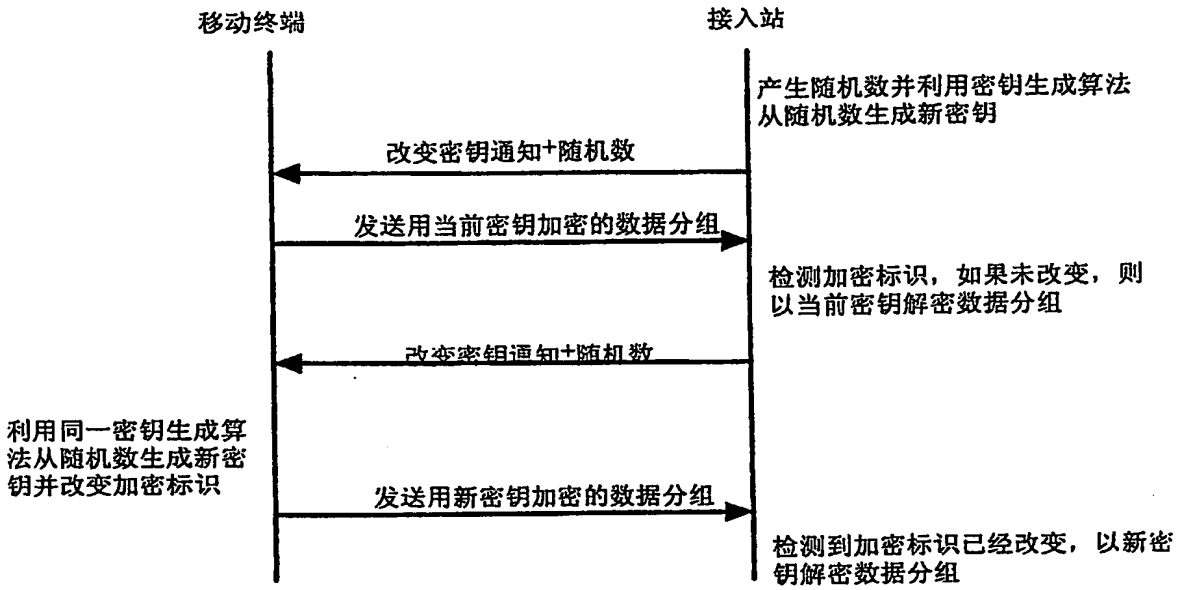

移动终端
接入站
产生随机数并利用密钥生成算法从随机数生成新密钥
改变密钥通知+随机数
发送用当前密钥加密的数据分组
检测加密标识，如果未改变，则以当前密钥解密数据分组
改变密钥通知+随机数
利用同一密钥生成算法从随机数生成新密钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密钥解密数据分组

图 3a

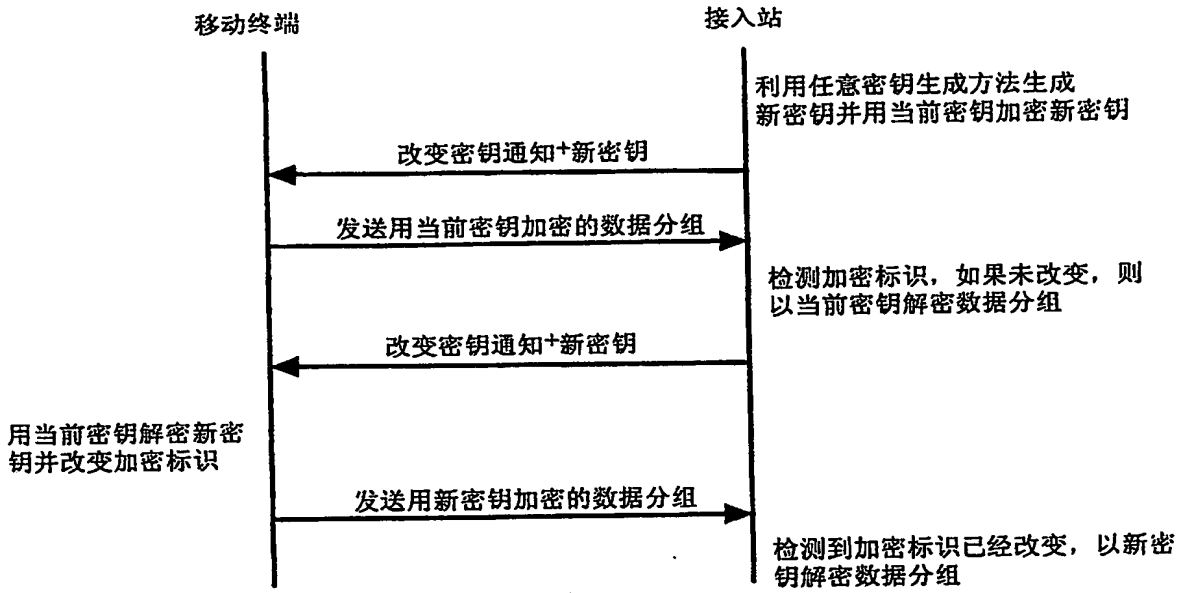

移动终端
接入站
利用任意密钥生成方法生成
新密钥并用当前密钥加密新密钥
改变密钥通知+新密钥
发送用当前密钥加密的数据分组
检测加密标识，如果未改变，则
以当前密钥解密数据分组
改变密钥通知+新密钥
用当前密钥解密新密
钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密
钥解密数据分组

图 3b

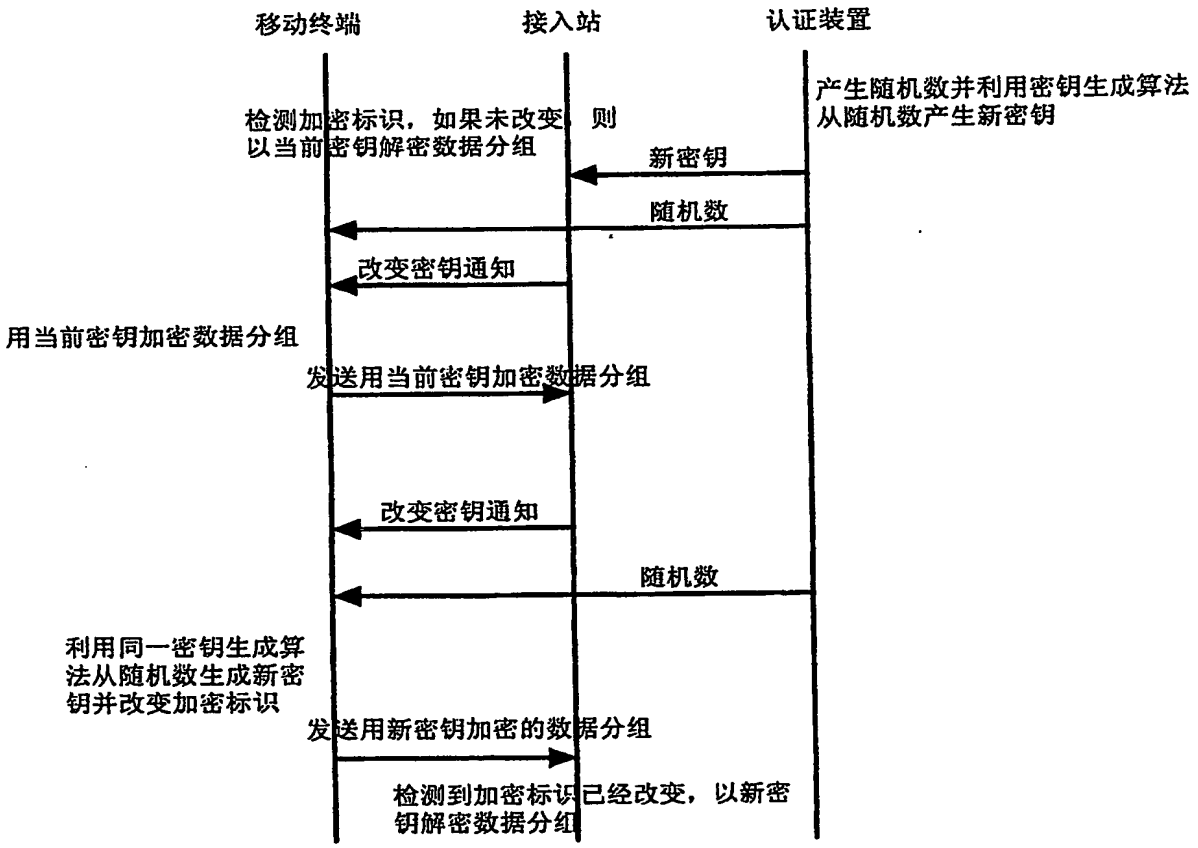

移动终端
接入站
认证装置
产生随机数并利用密钥生成算法从随机数产生新密钥
检测加密标识，如果未改变，则以当前密钥解密数据分组
新密钥
随机数
改变密钥通知
用当前密钥加密数据分组
发送用当前密钥加密数据分组
改变密钥通知
随机数
利用同一密钥生成算法从随机数生成新密钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密钥解密数据分组

图 3c

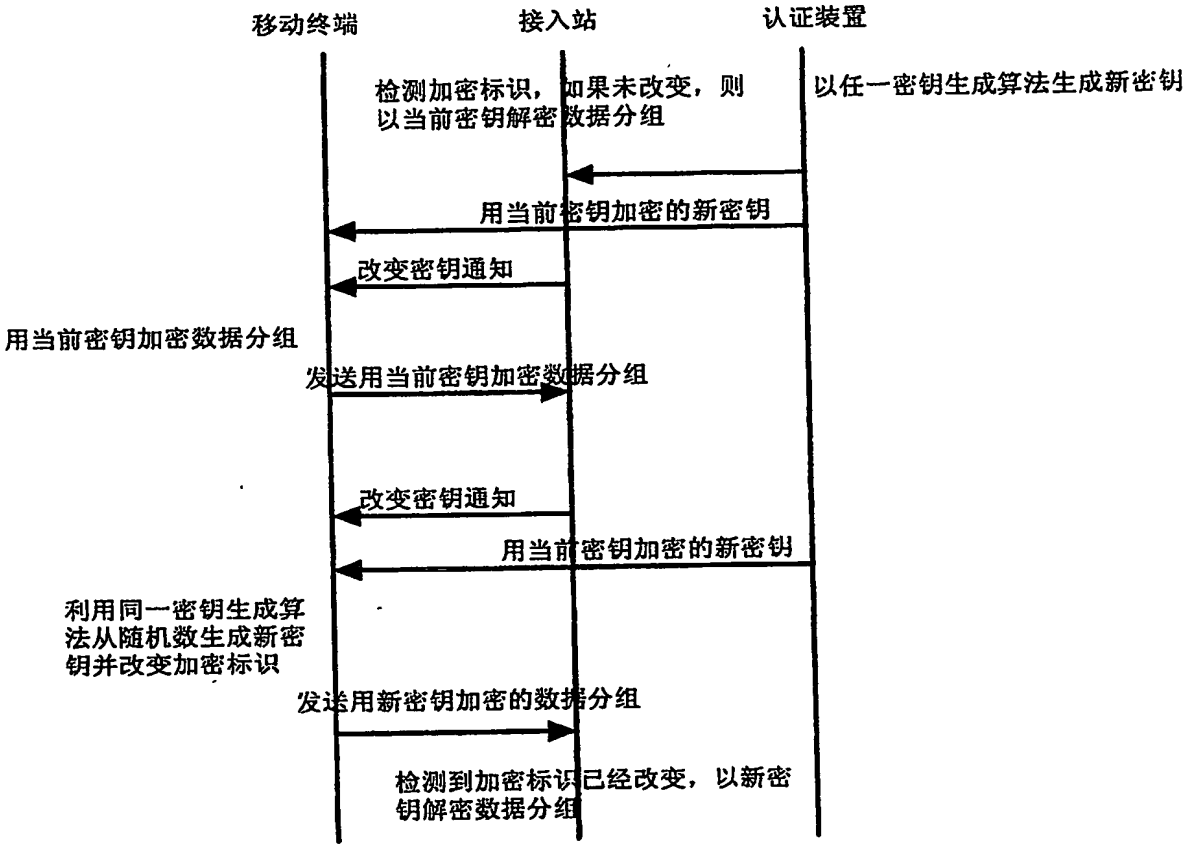

移动终端
接入站
认证装置
检测加密标识，如果未改变，则以当前密钥解密数据分组
以任一密钥生成算法生成新密钥
用当前密钥加密的新密钥
改变密钥通知
用当前密钥加密数据分组
发送用当前密钥加密数据分组
改变密钥通知
用当前密钥加密的新密钥
利用同一密钥生成算法从随机数生成新密钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密钥解密数据分组

图 3d

第VIII(iii)栏 声明：有权要求优先权

声明必须与规程213条的标准语句一致；参见对于VIII、VIII(i)到(v)(概述)的说明和专门对于VIII(iii)的说明。如果不使用本栏，则请求书中不应包括此页。

关于申请人在国际申请日有权要求下面指明的在先申请优先权的声明，如果该申请人不是在先申请的申请人或在提交在先申请后，申请人的姓名进行了变更。(细则4.17(iii)和51之二.1(a)(iii))：

关于本国际申请

华为技术有限公司基于下列各项，有权要求申请号为No. 02110833.1的在先申请的的优先权。

（I）华为技术有限公司作为发明人李永茂、吴更石的雇主是有权的；

（II）本声明是对所有指定国的。

☐ 本声明下转声明续页中“续第VIII（iii）栏”。

第VIII(iv)栏 声明：发明人资格声明 （仅为了指定美国的目的）

声明必须与规程214条的标准语句一致；参见对于VIII、VIII(i)到(v)(概述)的说明和专门对于VIII(iv)的说明。
如果不使用本栏，则请求书中不应包括此页。

发明人资格声明(细则4.17(iv)和51之二.1(a)(iv))
为了指定美国的目的：

我在此声明我相信我是要求保护和寻求专利的主题的原始、最初和唯一的（如果只列出了一个发明人）或者共同的（如果列出了不只一个发明人）发明人。

本声明是本国际申请的一个组成部分（如果本声明与国际申请一起提出）。

本声明是关于PCT/_____号国际申请的（如果本声明根据细则26之三提出）。

我在此声明我的居所，邮寄地址，和国籍和列在我名字下面的一样。

我在此声明我已检查过并理解上述国际申请的内容，包括所述申请的权利要求书。在所述申请的请求书中，我按照PCT细则4.10写明了对外国优先权的任何要求，并且在下面的"在先申请"栏目下，通过申请号，国家或世界贸易组织成员，申请的日、月、年，我写明了向美国以外的国家提出的，其申请日早于所要求的外国优先权申请的申请日的任何专利申请或者发明人证书申请，包括指定至少一个除美国以外的国家的任何PCT国际申请。

在先申请：申请号：**02110974.5** 申请日：**020308**

发明名称：无线局域网加密密钥的分发方法

我在此承认自己有义务公开我知道的，根据美国联邦法规（CFR）第37篇第1.56条对确定专利性有实质意义的信息，包括对于部分继续申请，在该在先申请的申请日和该部分继续申请的PCT国际申请日之间可得到的实质性信息。

我在此声明所有根据我自己的知识所作的声明是真实的，并且所有根据信息和相信所作的声明相信是真实的；而且在作这些声明时我知道根据美国法典第１８篇第１００１条故意作假声明以及有关类似行为将受到罚款或监禁或二者并罚的惩罚，并且这样的故意假声明将危害申请或根据该申请授予的任何专利的有效性。

姓名：李永茂

居所(城市和美国的州(适用时)，或国家)：中华人民共和国

邮寄地址：中国广东省深圳市南山区科技园科发路华为用服中心大厦 邮编：518057

国籍：中华人民共和国

发明人的签字：李永茂 日期：2003年1月24日

（如果签字未包括在请求书中，或如果声明是根据细则26之三在提出国际申请之后更正或增加的。该签字必须是发明人的签字，而不是代理人的签字）

（如果签字未包括在请求书中，或如果声明是根据本细则26之三在提出国际申请之后更正或增加的，该签字必须是发明人的签字，而不是代理人的签字）

姓名：吴更石

居所(城市和美国的州(适用时)，或国家)：中华人民共和国

邮寄地址：中国广东省深圳市南山区科技园科发路华为用服中心大厦 邮编：518057

国籍：中华人民共和国

发明人的签字：吴更石 日期：2003年1月20日

（如果签字未包括在请求书中，或如果声明是根据细则26之三在提出国际申请之后更正或增加的。该签字必须是发明人的签字，而不是代理人的签字）

（如果签字未包括在请求书中，或如果声明是根据本细则26之三在提出国际申请之后更正或增加的，该签字必须是发明人的签字，而不是代理人的签字）

☐ 本声明下转声明续页中“续第VIII（iv）栏”。